Fraud Prevention Toolkit: Self-Assessment

This assessment is for educational purposes only. It may assist you with identifying your potential vulnerabilities to scams and provide you with tips on how to reduce those vulnerabilities. This assessment does not include every possible action that can be taken to reduce someone's risk to scams and does not guarantee that you may not fall victim to a scam. You know best what actions may work best for you and other educational resources may also meet your needs.

Response Assessment

The Response Assessment is a series of questions that may help identify strengths and weaknesses in your natural responses to certain situations that could impact your risk towards scams.

How likely are you to automatically trust an authority figure (e.g. law enforcement, attorney, etc.)?

○ Not Likely ○ Not Sure ○ Likely

How likely are you to automatically trust a message or website based on a well-known logo/name (e.g. Amazon, Apple, Microsoft, etc.)?

○ Not Likely ○ Not Sure ○ Likely

How likely are you to trust a friend or romantic interest that you met online?

○ Not Likely ○ Not Sure ○ Likely

How likely are you to share financial information with an actual or perceived friend or family member?

○ Not Likely ○ Not Sure ○ Likely

How likely are you to send someone money that you care about due to a hardship without confirming the request (e.g. medical emergency, legal fees, etc.)?

Not Likely | Not Sure | Likely

How likely are you to follow someone's direction if someone attempts to extort or threaten you (e.g. threat of arrest, exposure of sensitive information, etc.)?

Not Likely | Not Sure | Likely

How likely are you to act quickly due to perceived urgency (e.g. limited time deal, a message that your computer or account is compromised, etc.)?

Not Likely | Not Sure | Likely

How likely are you to ignore red flags in lieu of the possibility of a prize or some perceived benefit?

Not Likely | Not Sure | Likely

How likely are you to research a website, business or person whether recognized or not prior to providing money, financial information or personal information?

Not Likely | Not Sure | Likely

How likely are you to report a scam to a reporting agency or law enforcement?

Not Likely | Not Sure | Likely

Security Assessment

The Security Assessment is a series of habit statements that by responding to each statement can provide you with a general assessment of the areas where you are taking security precautions to prevent scams and opportunities that may help reduce your risk of scams.

Trusted Contacts

I have trusted contacts that can help me identify scams.

◯ Yes ◯ No

I have a unique code word that I have shared with my close friends and family members, so I can confirm their identity through electronic communications or over the phone.

◯ Yes ◯ No

I have a trusted person as a joint owner on my financial account(s) to assist me in the event I am unable to manage my account for a period of time.

◯ Yes ◯ No

Physical Security

I secure personal identifying documents in a fireproof safe when not in use (e.g. social security card, birth certificate, etc.).

◯ Yes ◯ No

I secure my physical account number(s) and debit/credit card(s) in a fireproof safe when not in use.

◯ Yes ◯ No

I shred mail or documents that have my personal identifying information or contact information listed that do not need to be retained.

◯ Yes ◯ No

I do not share my account numbers, debit/credit cards or PIN with others, including family members.

Yes No

I have a list of all the financial institutions' phone numbers I do business with.

Yes No

I have a list of all my debit or credit card lost/stolen phone numbers.

Yes No

I check a card payment terminal for unusual skimming, shimming, other foreign attached devices or tampering before using my card.

Yes No

I check all of my financial accounts daily.

Yes No

I monitor my credit report regularly.

Yes No

Communications

I screen calls from phone numbers that I do not recognize.

Yes No

I do not respond to unexpected text messages, calls or emails.

Yes No

I reach out to a person, business or government agency directly instead of using a phone number or link listed in a communication.

Yes No

I do not call phone numbers or click on links on unexpected pop-up messages despite the message's content.

Yes No

I do not click on links in emails or text messages that were unexpected.

Yes No

Device Security

I password protect all of my electronic devices (e.g. cell phone, tablet, computer, etc.).

Yes No

I keep all my devices' software updated.

Yes No

I do not share my device passwords with others, including family members.

Yes No

My home Wi-Fi network is secured.

Yes No

I do not allow others into my devices that store my digital wallet and/or mobile banking application.

Yes No

I do not scan unusual or unexpected QR codes with my devices.

Yes No

I do not use public or free Wi-Fi on my devices.

Yes No

I have security monitoring software on all electronic devices connected to the Internet.

Yes No

Online Safety

I do not share my online banking login credentials with others, including family members.

Yes No

I only enter my account or card number information into online accounts that are in my name.

Yes No

I enter a web address instead of searching for a website through a search engine.

Yes No

I use reputable sources to research websites or information before supplying my personal or financial information.

Yes No

I read through return policies and product/service descriptions fully before making a purchase.

Yes No

I understand that the terms "free trial" when associated with a product or service typically mean that I will be enrolled in a subscription if not cancelled or charged if a product is not returned.

Yes No

I keep a list of all websites that may store my personal or financial information.

Yes No

I delete online accounts or remove my personal or financial information from accounts I no longer use.

Yes No

I have set up Google Alerts to monitor my name to notify if my name becomes listed online without my permission.

Yes No

I keep my social media profiles and all posts private.

Yes No

I keep my personal identifying information off my social media profiles.

Yes No

I do not accept friend requests from individuals I do not know or that seem suspicious on social media sites.

Yes No

I do not respond to messages from contacts I do not know or that may be pretending to be someone I know through social media sites.

Yes No

I research mobile/device applications before downloading, and I delete my accounts and uninstall applications if I no longer use them.

Yes No

I use different passwords for every account.

Yes No

I use strong passwords that are random (i.e. at least 16 characters long, including upper case letters, lower case letters, numbers, special characters).

Yes No

I keep my passwords in a password manager instead of writing passwords down on paper.

Yes No

I turn on multi-factor authentication for all accounts that offer it.

Yes No

I use a credit card instead of a debit card when shopping online.

Yes No

I use digital wallet payment options when possible to protect my card information.

Yes No

Education and Reporting

I regularly stay informed of red flags of scams through the Federal Trade Commission, Michigan.gov, Federal Bureau of Investigation or other reputable resources.

Yes No

I regularly stay informed on cybersecurity best practices that relate to the technology I use through reputable resources.

Yes No

I report lost or stolen account numbers or cards, or unauthorized transactions immediately to my financial institution.

Yes No

I report scams or fraud to the appropriate channel or government agency, etc.

Yes No

I report phishing emails and smishing text messages (i.e. scam emails or text messages).

Yes No